1983-06

Disaster planning for Navy ADP systems.

Hickman, John Randall.

Monterey, California. Naval Postgraduate School

nterey, CA 93943

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

DISASTER PLANNING FOR NAVY ADP SYSTEMS

by

John Randall Hickman

June, 1983

Thesis Advisor: John R. Hayes

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER
2. GOVT ACCESSION NO.
3. RECIPIENT'S CATALOG NUMBER

4. TITLE (and Subtitle)
Disaster Planning for Navy ADP Systems

5. TYPE OF REPORT & PERIOD COVERED
Master's Thesis
June, 1983

6. PERFORMING ORG. REPORT NUMBER

7. AUTHOR(s)
John Randall Hickman

8. CONTRACT OR GRANT NUMBER(s)

9. PERFORMING ORGANIZATION NAME AND ADDRESS
Naval Postgraduate School
Monterey, California 93940

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS

11. CONTROLLING OFFICE NAME AND ADDRESS
Naval Postgraduate School
Monterey, California 93940

12. REPORT DATE
June, 1983

13. NUMBER OF PAGES
64

14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)

15. SECURITY CLASS. (of this report)
Unclassified

15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)
Approved for Public Release, Distribution Unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)
Disaster Planning, Contingency, ADP, Department of the Navy,
Risk Analysis

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

ADP systems have become vital to many Navy activities and thus have created a need for disaster planning which will ensure the continued operation of these systems. However, disaster planning is expensive, long-drawn, and difficult to implement under day-to-day operational commitments.

This study analyzes the directives governing Navy ADP disaster planning, presents affordable alternatives, and suggests the need for a Navy support team to assist in the implementation of disaster plans.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

Approved for public release, distribution unlimited

Disaster Planning for Navy ADP Systems

by

John Randall Hickman
Lieutenant, United States Navy
B.S.E., University of Pennsylvania, 1978

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
June 1983

ABSTRACT

ADP systems have become vital to many Navy activities and thus have created a need for disaster planning which will ensure the continued operation of these systems. However, disaster planning is expensive, long-drawn, and difficult to implement under day-to-day operational commitments.

This study analyzes the directives governing Navy ADP disaster planning, presents affordable alternatives, and suggests the need for a Navy support team to assist in the implementation of disaster plans.

TABLE OF CONTENTS

I. INTRODUCTION

Although Automatic Data Processing (ADP) systems are becoming so vital to the very existence of many Federal activities, there has been surprisingly little preparation for the event of a sudden disaster which might annihilate both the system and the essential decision-making capability provided. This paper will analyze some of the options available to provide contingency planning for such disasters. It is shocking to see the types of organizations that would be rendered useless and the chaos that would result if their systems were damaged by a disaster. In this discussion, the term "disaster" will refer to major fires, storms, flooding, sabotage, theft, power loss, air conditioning failure, or even personnel actions such as strikes, terrorism, etc. which exceed a critical time limit. This is to differentiate from a computer outage, which generally lasts a short, tolerable time.

Organizations have generally been most interested in getting new systems on line as quickly as possible and integrating them into the main stream of day-to-day business. This has created a dangerous level of dependence on computers to the point of threatening extinction for the organization should the computer be eliminated. The problem

is that in the haste to get these computers operational, an important issue has been overlooked--disaster planning. In most cases, disaster planning is an afterthought and occurs at a time when a tremendous effort is necessary just to figure out what applications are important to the organization. There are indications which suggest that in the Navy, not only is disaster planning an afterthought, but it is often "sitting on the back burner" waiting for a disaster to prove its worth. Despite numerous cases of computer centers being wiped out by disaster, too many data center managers believe that it won't happen to them. What if it did ? Are Navy ADP facilities prepared to handle major disasters? Are there adequate guidance and specific directives which ensure preparedness? If a specific Navy ADP center is not qualified or capable of preparing its own disaster plan, who may it contact for assistance? What contingency options are available? These critical questions will be addressed in subsequent chapters.

II. BACKGROUND

A. GAO STUDY ON CURRENT STATE OF PREPAREDNESS

In a report to the Congress dated 18 December 1980, the General Accounting Office (GAO) claimed that most federal agencies "have not developed adequate ADP backup plans to minimize disruption of their ADP systems and maintain continuity of operations in an emergency." [1] In a review of 55 federal activities, GAO did not find one ADP backup plan which it considered adequate. This is quite astounding evidence that either current directives on disaster planning are too weak to enforce, or they are not fully understood by the federal agencies. Do ADP managers actually believe that they are complying with contingency planning requirements? According to the GAO, federal agencies have placed far less importance on ADP backup than commercial organizations have. Why is this so? Obviously, a commercial activity is at risk of going out of business should its computer system fail. Its profits are linked to the information processing capability, so it is easy to justify the cost of disaster planning as a type of insurance. Its long term benefits outweigh the initial cost. The Navy on the other hand, does not believe in insuring computers, and has quite a different set of objectives. In the government, the head of each

agency is responsible for its continued existence, and therefore the Office of Management and Budget (OMB) has directed in its circular A-71 Transmittal Memorandum 1 (dated July 27,1978) that "the head of each executive branch department and agency is responsible for assuring an adequate level of security for all agency data." Such a security program must include:

1. Periodic risk analysis to determine vulnerability and minimize potential for loss.
2. Establishment of an appropriate contingency plan to insure continuity of operations should a disaster occur which would interrupt normal operations.
3. A periodic review and test of contingency plans.

The GAO believes that these OMB requirements are not being properly enforced and that high level management is not acting to prevent major loss of ADP capability through contingency planning. In most cases, proper risk analysis has not been made to determine the impact of lost ADP systems and even when it has, the contingency plans are inadequate. The problem is compounded by conflicting requirements placed upon agencies, budgetary constraints (reliable backup is very expensive), and a lack of clear authoritative guidelines. Contingency planning is too often dealt with as a subsidiary of security discussions, and must be brought to the forefront in ADP acquisition and management as a critical issue.

Commercial facilities are currently available to specifically handle disaster backup and are utilized by private

industry. Several firms have even cooperated to build their own backup facilities and thus reduce costs by sharing expenses. Why can't Navy ADP activities do the same?

B. COMPUTER CENTER MANAGERS' POINTS OF VIEW

My interviews with several Navy computer center managers have indicated that indeed these managers believe they are personally responsible for ensuring that their disaster plans are adequate. However, they do not see any evidence of enforcement of disaster planning requirements. Although stated in the Department of the Navy's ADP Security Program Manual (OPNAVINST 5239.1A, Chapter 7 and Appendix J), minimum disaster planning requirements are difficult to ascertain because so much is left to the discretion of Commanding Officers [2]. Many managers feel that a reciprocal agreement with another Data Processing Center (see chapter V-C-1 for explanation of these agreements) is adequate for backup. GAO does not feel that these constitute valid backup plans. Certainly they can not be proven valid unless tested on a regular basis. OPNAVINST 5239.1A covers the requirement to annually test and evaluate a contingency plan (ch.7,pg.6), but the directive is very weak. It states,

> "Testing can be as extensive as transferring the entire ADP operation to an off-site facility or as minimal as conducting a fire alarm test. The depth and scope of the

operational testing is dependent upon the practicality and importance of demonstrating that the plan works."

This leaves quite a bit up to the discretion of the data processing center manager and the Commanding Officers of DP activities. As long as the Designated Approving Authority (DAA), the superior responsible for approving the ADP security program, is satisfied, a contingency plan which relies upon a reciprocal agreement may be accepted and may require little or no testing.

How then can the ADP manager be sure that his contingency plan will ever work? Testing and evaluation of the plans are often limited by budget constraints even though the activity is directed to plan and budget for regular testing. These budget constraints will become even more apparent when Navy Regional Data Automation Centers (NARDACS)[1] begin operating under Navy Industrial Funding [2] this year. Who will pay for the costs of a contingency plan at NARDACS? Is this an overhead expense to be passed on to

---

[1]NARDACS are regional data processing service centers established by the Navy to provide computer support to Navy activities in the area. This regionalization is purported to reduce duplication of effort and provide economies of scale to smaller activities which might not be able to operate their own centers.

[2]Navy Industrial Funding as applied to NARDACS, is action to make them operate as profit centers in competition with commercial DP contractors. This will necessitate use of accurate chargeback policies so that they can completely cover the costs of operation (they will not necessarily show a profit, but merely break even).

the customer? Another critical issue is how can a service agency such as a NARDAC develop a contingency plan that fits into a customer base of widely varying needs and diverse mission objectives. Before delving into these stimulating questions, it is necessary to lay the foundation of what goes into a contingency plan. The next several chapters will discuss the government's dependence upon computers, outline the need for ADP security, and then present details for developing a contingency plan.

III. GOVERNMENT DEPENDENCE ON COMPUTERS

As a matter of background, it is interesting to note the level of dependence our government has come to place upon computers. The capacity of modern day computers for reducing mountainous volumes of work has made them a mainstay in such organizations as the Bureau of the Census and the Social Security Administration (SSA). Consider that prior to 1890, through purely manual calculation, it took seven to nine years to just count the population of 70 million. Today it takes less than a year to compile a census for over 200 million people plus provide useful statistical data on labor, the economy and hundreds of other studies.[3] Although the magnitude of the census system makes it invaluable, the consequences of losing it for a few weeks would be nothing compared to the SSA's operation. The Social Security act of 1935 made it necessary to maintain employment records on all working people and established one of the world's biggest bookkeeping jobs. The SSA maintains about a trillion records and pays out over 100 billion dollars in benefits.[4] Imagine the chaos and personal hardship if these checks didn't get out on time. The manipulation of huge volumes of data originally caused the computer to be rooted in government operations. The

situation has long since nullified the option to shift to the manual processing mode in an emergency.

This however, is only one problem. The centralization of data resources has made vital information dangerously susceptible to a catastrophic loss. The rapid growth of the United States, and the government's involvement in maintaining data on its population for tax purposes, benefits, resource management, etc. have made the computer an indispensable tool. While federal employment has leveled off since the 1970's, the number of computers in use in the government has increased by an order of magnitude.[5] Have computers taken the place of federal employees? Perhaps, but they have also relieved them of some mundane clerical jobs. A GAO study indicates that computers have enabled the government to do its work with 600,000 less employees in 1980 than would have been required without computers.[6] Computers have made us more efficient and have established this efficiency as a standard way of life. Could we return to the old inefficient ways if computers were taken out of action? Probably not! The state of affairs has come too far, and many automated applications today were never done manually to begin with.

Given the demonstrated dependence on computing, the need for protecting Automatic Data Processing (ADP) resources is obvious.

IV. THE NEED FOR ADP SECURITY

A. VULNERABILITY OF CENTRALIZED DATA

Would you trust the most valuable secrets of your company to a stranger who walked in from the street ? Would you leave your most detailed financial reports, customer listings, and manufacturing cost summaries lying around the front lobby? Would you print everything necessary for stealing or ruining your organization in the daily newspaper, or set yourself up to be taken hostage? Not intentionally of course, but that is exactly what you are doing by entrusting all of this information to a computer without a thorough information security plan. Although most ADP managers realize the need for information security, they rarely comprehend the vulnerability of their systems, and they fail to understand the actual value of computing resources to the survival of their organizations.

The topic of computer and information security is much too broad in scope for complete coverage in this paper, but a thorough discussion of disaster planning must include security considerations and if nothing else, a few horror stories and security foulups to emphasize the necessity for comprehensive contingency planning.

Before the advent of microcomputers and prior to the hardware revolution of the 1970's (which brought the price

of hardware down dramatically),[3] maintaining a corporate database was expensive (in the millions of dollars range). The most economical means of keeping a vast amount of information was through a centralized database. The most economical means of computing in general was to put all of the expensive resources in one place and share them as widely as possible. In most cases it was clearly too costly to give branch offices their own computers. Centralization was appealing for numerous reasons:

1. It facilitated corporate management level control over resources.
2. Centralized ADP support staff (less people, less duplication of effort, greater concentration of expertise).
3. Consistent maintenance and operations standards for hardware and software.
4. Planned, controlled growth.

These appealing features have created a belief that centralization is always good. They have also clouded the fact that centralization of databases and ADP resources is a dangerous practice which makes the organization unacceptably vulnerable to ADP disaster (unless a valid disaster recovery plan is in effect). References on distributed systems[4] make

---

[3]For discussion on hardware pricing trends, see Ref. [23]

[4]See Harold Lorin, reference [24].

convincing arguments that distributed computer systems can be an economical and safe (secure and well backed up) alternative to centralization. This point will be discussed in section V-C-2 under Recovery and Backup Plans.

When an entire organization becomes dependent on its computing resources to the extent that denial of such resources would put it out of business, security had better be a paramount consideration. Additionally, many managers fail to realize that there are legal requirements to protect company assets and that failure to do so is criminal negligence. The Foreign Corrupt Practices Act (FCPA) of 1977 requires that corporate officers "maintain accountability for assets [and that] access to assets is only permitted in accordance with management's general or specific authorization." [7] Individual penalties for top executives can reach ten thousand dollars and five years imprisonment (in cases where such assets are lost or destroyed due to negligence).[8] These assets include hardware, software, and information (data and documents). The FCPA is even more specific about accounting procedures and mandates detailed record keeping of transactions. If these functions are performed by computer, they absolutely must be traceable, reproducible, and in accordance with accepted accounting principles. This requires that valuable records (computer files, tapes, etc.) be protected against fire, flood, sabotage, and any other disaster imaginable.

Aside from the legal requirements, if managers intend to keep the business going in the face of disaster they had better enforce a policy on disaster planning. It is a sad reality that most users of computing resources don't realize the value of their system until they are denied its use or until they are charged for it. Whatever the current cost (charge), it would be considered inexpensive if compared to a reconstruction effort in the aftermath of a disaster; but this need not be the case if such a contingency has been prepared for.

B. MAGNITUDE OF COMPUTER-MADE DECISIONS, IMPLICATIONS OF POSSIBLE ERRORS AND LOSS

It isn't necessary to delve into much detail on the magnitude of computer-made decisions; however, it is noteworthy that such decisions are increasing at an alarming rate. Computers are in charge of shipping and ordering supplies, controlling critical machinery, sending out payrolls, generating invoices, ordering services , and in general making billions of dollars worth of decisions , often with neither human review nor intervention [9]. This is a trend that has made organizations vulnerable to extreme losses from both computer errors and complete disaster to the computing resources.

A University of Minnesota study showed drastic decline in business activity as ADP outage continues over time.[10]

Within one week most automated activities cease to function altogether. Financial loss which occurs and loss of customers is often beyond restoration.[5] How does this apply to Navy ADP facilities where profit is not necessarily an organizational objective? Although the profit motive may not necessarily exist, Navy Industrial Funding (NIF) requirements will force Navy Regional Data Automation Centers (NARDAC) to at least break even. Additionally, there is ample evidence supporting the need for uninterrupted ADP operations in terms of minimizing cost to the taxpayers, and in terms of accomplishing the Navy's or DOD's mission. Examples of this exigency include:

1. Vital Tactical Systems

Vital Tactical Systems such as the Worldwide Military Command and Control System (WWMCCS) are particularly complicated disaster recovery scenarios due to security considerations and the specialized nature of their applications. This paper is concerned with more general ADP operations and therefore tactical systems will not be discussed further.

---

[5] One Washington D.C. area bank who is a member of Bancon, Inc. lost over $30,000 in interest over a 24 hour outage - Ref.[6]; An airline reservation system manager indicated that it costs the airline over $300,000 through lost reservations each time their ADP system goes down - Ref.[16].

2. Logistics and Supply Support for the Navy

These systems make the Navy susceptible to both monetary loss and reduction in mission capability. Repair parts are necessary to keep our combat forces in action and a supply center computer disaster could be a serious threat to combat readiness. It certainly would slow down supply operations to an unbearable level. Think of how valuable the database must be and consider the implications (in manhours and dollars) of reproducing it. In some cases it would be impossible to replace in the event of a disaster. The magnitude of controlling parts inventory and supplies (over 3.5 million items of supply valued at $200 billion [11] is such that we could no longer hope to fall back on manual methods and therefore are obligated to guarantee the continued operation of ADP centers.

3. Navy Payroll

Finance and payroll systems are an invitation for financial chaos in the event of computer disaster. Disruption of the pay system would also create impossible morale problems if paychecks were not distributed on time. If records were destroyed, there would be an unbelievably complex reconstruction effort necessary in order to regenerate the lost data, and there would be a great exposure to possible fraud.

4. Navy Regional Data Automation Centers

These service centers are entrusted with processing data for numerous Navy customers. It is unlikely that their customers have prepared for a computer disaster, and it is incumbent upon the NARDAC to provide not only protection for data, software and hardware but some assurance of continuity in operations. In reality, disaster planning should be conducted by all parties in this scenario in order to determine critical applications and the extent of damage possible due to computer outage. This topic will be discussed further in chapter VI under Applicability of Disaster Planning to Navy ADP.

In addition to financial, organizational, mission-degrading, and morale problems, there are situations where human life is threatened by computer disasters. This is usually a clearly recognized risk in systems which control machinery, nuclear power plants, air traffic, and hospital life support systems and hopefully a valid disaster recovery plan is in effect. Government regulatory agencies and auditors are very concerned in these cases and generally mandate a disaster plan. The implications of a computer disaster are serious and the following chapters will discuss how the consequences can be minimized and how best to prepare for them.

V. CONTINGENCY PLANNING

If the previous arguments have not been convincing enough to encourage contingency planning, the next will be--contingency plans are required by law for most Navy ADP operations. Specific directives and their applicability will be covered in chapter VI. Now that the importance of contingency planning has been shown, how does one go about implementing such a plan?

A. RISK ANALYSIS

The first and most essential step of a contingency plan is to conduct a thorough risk analysis. Federal Information Processing Standards (FIPS) Publication 31 [12] gives quite detailed procedures for carrying out risk analysis and cites three major categories with which to deal--loss potential estimate, threat analysis and annual loss expectancy.

1. Loss Potential Estimate

This phase involves identifying the data center's assets and assigning a value to them. Critical applications must be determined and a priority scheme established. The operations manager should know this scheme in order to carry out his daily functions. In dealing with scheduling and in coping with minor outages the operations staff should have a feel for which jobs are most critical. But do they

know which people are most critical or what data files are important?

a. Assets

The following categories of assets must be considered in terms of their replacement costs (in dollars), the time period required to replace them, the specific applications upon which they impact, and the criticality to mission accomplishment:

1. Personnel
2. Hardware
3. Software
4. Data/Information
5. Documentation/Operations Procedures
6. Facilities/Power/AC
7. Supplies (especially difficult to procure items such as personalized checks, customized forms, etc.)
8. Telecommunications

b. Loss

The term "loss" in reference to ADP assets can be interpreted in varying degrees. It need not necessarily mean total destruction but rather could refer to:

1. Denial of the resource, e.g. computer center held hostage, tape library index sabotaged, etc.
2. Modification (intentional or not) e.g. systems programmer changes code to defraud a payroll system
3. Disclosure, e.g. valuable database revealed to competitor
4. Theft

Although a proper risk assessment will address these varying degrees of loss and quite correctly assign different potential loss values accordingly, one will find that modification, disclosure, and theft are more of security considerations than disaster planning. Since the objective of this paper is to analyze disaster planning, the term "loss" will be used in the context of computing resource destruction and or denial.

c. Priority

The first step of the loss potential estimate identifies assets. The next step involves prioritizing them so that proper protection and backup can be afforded to the high priority items. An example of priorities would identify critical time limits for each asset loss as follows:

1. Loss of this equipment/capability for more than some acceptable number of hours could seriously damage the organization.
2. Loss of this equipment for more than some acceptable number of days would be serious.
3. Loss of this equipment for more than some acceptable number of weeks/months would be serious.
4. This equipment/capability is non-essential and may be replaced at earliest convenience.

Obviously, the highest priority (number 1) items would be the first to bring up in the recovery phase of a disaster. They may in fact be the only ones possible to bring up quickly with the limited resources available following a

disaster. As recovery progresses the lower priority items would be brought up.

2. Threat Analysis

It will be necessary to determine which threats pose the most serious damage to the system. For example, one might consider the threat of earthquakes because of a location in California, whereas a location in Florida would not be concerned (For them, hurricanes would be threatening.) Probability can be assigned to these risks through the the aid of such services as the National Earthquake Information Center, the National Weather Service, and by using historical data. FIPS publication 31 provides a very thorough list of threats to consider and who to contact for further information. [12] Included in this list are the following:

a. Unauthorized access

(1) Theft
(2) Arson
(3) Vandalism
(4) Tampering
(5) Circumvention of Internal Controls

b. Natural Disasters

(1) Floods
(2) Storms
(3) Earthquakes
(4) Fires

c. Proximity hazards

(1) Chemical, petroleum, explosive operations
(2) High crime areas
(3) Airports (this hazard is a real concern for Fleet Numerical Oceanographic Center, Monterey and the Naval

Postgraduate School, both of whom are in the flight path of Monterey Airport).

d. Failure of Supporting Utilities

(1) Electricity
(2) Air conditioning
(3) Telecommunications
(4) Elevators
(5) Transportation system

e. Nonavailability of key personnel

(1) Hostage
(2) Accident
(3) Quitting
(4) Strike

f. Hardware failure

Not all of these threats will be applicable to each computer operation, but probabilities of occurrence will indicate which ones to worry about. Preventive measures which can be taken to reduce these risks will be discussed is section V-(B).

3. Annual Loss Expectancy

Combining the loss potential estimate and threat analysis (probabilities) will produce a basis for determining what is reasonable to spend on security measures for each asset. That is, multiply the loss potential by the probability of occurrence to obtain an annual estimate of the loss. Since probabilities are not always easy to generate, all estimates should be viewed cautiously and should be subjected to a sensitivity analysis to determine their ruggedness.

The level of detail described in this discussion is quite superficial and is not indicative of the level of effort involved in risk analysis. Risk analysis is time-consuming and tedious, but it is perhaps the most crucial step of disaster planning since it lays the foundation for future action.

B. PREVENTIVE MEASURES

"The most overlooked part of a disaster is avoiding it" [14]. In conjunction with the risk analysis, it is prudent to undertake certain preventive measures which will reduce the exposure to risk.

1. Controlling Access

Unauthorized access can be controlled through physical barriers such as "man-traps", walls, locked doors, fences, guards, electronic monitoring devices, and security badges. The best way is to physically secure the computer and vital resources and lock unnecessary personnel out.

2. Natural Disaster Preparation

Natural disasters are more difficult to control; however, structural engineers and architects can assist in designing sturdy earthquake resistant [15], storm resistant, and fire retardant buildings. Installed CO_2, Halon 1301, sprinklers and portable fire extinguishers will significantly reduce fire hazard if personnel are properly trained to use them. This means that fire drills and training should be a regular part of the data processing

operation. All personnel should be able to locate the proper valves and equipment in an emergency situation (particularly in the dark).

3. Avoiding Proximity Hazards

If possible, selection of the ADP center location should be made with these risks of natural disaster in mind as well as any proximity hazards (discussed in chapter V-A-2-c). There is not always the option of site selection, (particularly when the disaster plan is being set up after construction) so protection from these hazards is usually the best solution. Although one may not be able to affordably protect a building from disasters such as an airplane crash; vital information, documentation, tapes and software can be safely stored off-site to protect some of the assets.

4. Adequate Supporting Utilities

Failure of supporting utilities can be covered by such things as an Uninterruptable Power Supply (UPS) with generator backup, redundancy of equipment, vigorous preventive maintenance, and close monitoring of vital signs.

5. Protecting Personnel

One of the most valuable assets in an ADP operation is personnel. Some of the skills lost in a disaster would be irreplaceable, and it would be difficult to assign a dollar value to their worth. A small investment in training can go a long way in benefitting the overall security of the

organization. Often overlooked programs such as First Aid, Cardio-Pulmonary Resuscitation (CPR), and emergency drills can save precious lives during an accident or disaster (both on and off the job). Additionally, it is unwise to become dependent on a small number of individuals. It is inevitable in any organization that a few highly motivated individuals take it upon themselves to "know it all." These persons should be identified and encouraged to share their knowledge with the rest of the data center by writing documentation and conducting training. Personnel should be cross-trained to the maximum extent possible so that emergency personnel shortages can be filled expeditiously. This relieves the urgency that would result if one key man were missing. It also provides an enriched job environment for the employees, allows them to grow, and motivates them to take a personal interest in their data center. This has positive results on a day-to-day basis and prepares personnel for disaster recovery. A final recommendation about personnel is that an active recruiting program should be in effect. It is important to maintain contact with the job market and keep files on possible recruits. This will provide some depth which can be fallen back upon in an emergency.

6. Documentation

As mentioned previously, documentation can be a valuable tool for training but it is also invaluable in a

disaster recovery. The personnel, equipment, and environment may all be completely different in the aftermath of a disaster and good documentation may be the only way to bring the system back together. Therefore, it should be well written, easily understandable, up to date, and safely stored off site.

7. Hardware Reliability

There are several areas of preventive measures that deal with the hardware in an installation. First and most obvious is scheduled maintenance which must be carried out religiously in order to provide reliable equipment. High operational tempo should not be allowed to supersede preventive maintenance or else machine down time will seriously impact upon the DP schedule. Other preventive measures involve protecting the environment in which the machines operate. Ensure that the temperature remains cool and stable. If the equipment is exposed to possible water damage, provide equipment covers (something as inexpensive as rolls of polyethylene for a few dollars can save millions of dollars worth of computers from water damage from above.) Instruct operations personnel on the location of these covers, how to secure the computers, and what to do in minimizing water damage. Drills should be conducted frequently to ensure familiarity with these procedures.

8. Emergency Action Plan

In preparation for a disaster it is necessary to draw up a detailed Emergency Action Plan. This includes checkoff sheets for varying degrees of emergencies, with personnel assignments (by name) for actions to be taken in each possible situation. For example, a section describing actions to be taken during a fire might include:

--If small fire, attempt to extinguish with portable CO_2, at same time sound fire alarm.

--Shift supervisor: notify fire department (phone number xxx and secure equipment if necessary.

The plan should include who to contact, phone numbers, and the sequence of actions to combat the initial emergency. Obviously this plan must be kept up to date as personnel, numbers and equipment change, and it should be tested frequently to make sure that it works smoothly.

C. RECOVERY PLAN

The final part of the contingency plan will be a recovery plan to prepare for reconstruction and/or putting the system back on line. It may provide for a temporary installation to begin with and subsequent rebuilding of the facilities or numerous other alternatives discussed in the following sections. It is common to see organizations with little or no recovery plans at all. In these situations, the management may believe that the risk of disaster is so small that the cost for a recovery plan is not worthwhile.

In many cases they have got neither the time nor the money for such a plan and they intend to react in "the seat of the pants" mode when a disaster occurs. Interviews with the Data Center managers at the Naval Postgraduate School, Navy Regional Data Automation Center, San Francisco, and the County of Monterey Data Processing center have indicated that this is not an unreasonable alternative in their minds. They have faith that hardware vendors would go to extraordinary lengths to replace any damaged equipment as quickly as possible (to the extent of shipping the next computer to come off the assembly line or diverting one intended for somebody else). They believe that a staff of essential personnel could pull together the necessary details for re-assembling the computer center. This is simply too optimistic and a very easy escape from the cost involved in an adequate recovery plan. Since it would be politically undesirable to espouse a policy of having no disaster plan, most prudent data center managers have established some type of minimum plan; usually a reciprocal agreement with some other data centers. These reciprocal agreements can be an oral agreement or a written contract between two or more data centers which promise to provide backup facilities to the center which experiences a disaster.

1. Letters of Agreement

When reciprocal agreements are undertaken, the written contract is usually preferred over an oral agreement. In this way, most facilities can legally solve the requirement for data center backup. While such agreements may look adequate on paper, they seldom come close to being useful in the true disaster situation. John P. Murray, in his January 1980 Data Management article made the following comment on the sufficiency of letters of agreement, "While these are the least expensive methods (for disaster recovery) they are also the least effective." [16] There are numerous problems with this type of backup, the most probable of which is the fact that no two systems are going to be completely compatible. Even if the hardware suite is exactly the same, it is highly unlikely that the operating systems are the same. [6] Full compatibility requires continual update of the contingency plan to ensure that critical applications will run on the backup system. Realistically, it must be understood that most ADP centers simply do not have the excess capacity to provide backup for someone else during prime time. (The capacity may be available on the midnight shift, and if this is acceptable to the afflicted center, it may be a workable agreement.) If the center does have unplanned extra capacity, it is probably not operating its equipment very efficiently. The point is that even an operation operating at moderate

capacity would be placing itself into a contingency situation in the event of someone else's disaster. There is no guarantee that the backup facility will be willing to sacrifice its own operation because of another's misfortune, and the promised resources might not materialize as planned. If the resources were made available, the agreements usually have no specification as to length of time that backup will be provided. Obviously the backup center cannot operate for very long at a reduced capacity.

Finally, it is extremely difficult to test these contingency plans and keep them current. Only two of fourteen activities with letters of agreement, in the GAO study, had tested their plans within the past year [1]. Reasons for not testing them included lack of available funds and non-availability of the backup system. The conclusion is that letters of agreement are relatively useless as a sole means of backup; however, they may provide reasonable alternatives as part of a contingency plan as long as the following guidelines are adhered to :

--The backup center should have nearly identical equipment.

---

[6]Note: These agreements usually provide a certain amount of shared resources between the recovery center and the afflicted centers. This does not usually provide for the option of bringing up an entirely different operating system.

--The backup plan should be executed during slack time or on a computer with excess capacity. (In other words, the execution of the plan should not place the backup center in a disaster situation).

--The agreement contract should be specific as to amounts of processing time and duration of contingency operations.

--The agreement should provide for frequent test opportunities in order to keep it current.

2. Dual Systems and Distributed Systems

The concept of dual systems involves probably the most complete solution to computer backup by having two exact duplicate systems operational as backups for each other. This option is extremely expensive and is only justifiable in a few cases. It also has a number of major cost tradeoffs which may limit its effectiveness. Ideally the backup system would be completely idle, standing by for the occurrence of a disaster. This would probably not be justifiable and would realistically have applications being run on it to increase the cost effectiveness of the system. The tradeoff would involve ensuring that enough excess capacity was available to handle critical operations yet utilizing the system as efficiently as possible to justify costs. Increased utilization would jeopardize backup response, and better response would waste resources.

Another consideration is how to distribute operations personnel. If the backup system were in complete standby, the personnel needs would be minimal. As the

attempt to make efficient use of the backup facility increases, so does the need for personnel. This may necessitate wasteful duplication of effort in the two separate systems. One more problem would be the question of where to locate the two systems. Close proximity would limit personnel, maintenance, facilities and support costs but would make both systems susceptible to many of the same disasters. Separation would increase these costs yet provide more secure protection against disaster. As a final negative point about the dual systems concept, a GAO investigation [17] frowned upon the Air Force's proposal to implement such systems at several of its bases. The GAO felt that dual systems were not justifiable since the workload could be handled by a single large CPU. The Air Force had failed to present a strong argument based on disaster planning which would have been difficult for GAO to refute. Ironically GAO came out with a report one year later which criticized most Federal Agencies for lack of disaster planning [1].

Organizations which are willing to pay the enormous price of dual systems usually have a lot at stake when their computers go down. One example is Chemical Bank of New York, which established a second site operation 40 miles away from its main system. [18] With critical applications identified, they divided the load between the two systems and set up a plan to run on either system during disaster.

Another company, TOWLE Manufacturing Corporation which processes one thousand orders per day (including over 10,000 line items of Leonard Silver), has also set up a second site but intends to use it almost exclusively for backup. Since they couldn't justify a completely idle computer, they have carefully selected a few outside users to defray some of the expense. By carefully monitoring the usage so that enough reserve is available for Towle's critical applications, they have developed a very reasonable and secure backup system.

A reasonable extension to the idea of dual (or multiple systems) is the concept of distributed systems. This blossoming technology offers an economical means of sharing computing resources and may be a feasible solution to disaster planning very soon. The details, pros and cons of distribution will be left as a topic for future research.

3. Disaster Recovery Centers

Rather than undertaking to build a backup site on its own, an organization may opt to subscribe to a commercial Disaster Recovery Center. These come in two basic forms: a "shell site" or a "hot site."

a. Shell Site

A shell site is basically a place to go when one's computer center is annihilated. It contains no computers or peripherals, but has adequate chill water connections, air conditioning, raised floors, and power

sufficient to sustain a computer installation. Either the subscriber must provide the equipment when a disaster recovery is initiated, or in some cases the vendor assists in obtaining the necessary gear. These sites range widely in price depending upon the size of facilities, and what is included in the services. One company, DCI, provides the shell for $750/month membership fee with no disaster notification fee. However, if the disaster lasts over 90 days the occupant must pay $20,000/month thereafter. Another company, Data Processing Security Inc. of Fort Worth, Texas, charges an $84,000 fee for a minimum seven-year membership and $12,000 per year thereafter, plus a pre-specified amount per month during actual usage. This provides 18,000 sq. ft. of computer space with all necessary environmental support and 15,000 sq. ft. of office space.

The price can become quite steep and full recovery from the disaster is still dependent on how quickly the equipment can be obtained. If the current operation is using equipment that may be difficult to procure or that may involve a long lead time to acquire, it would be unwise to pay for a shell site which couldn't be used immediately due to lack of equipment.

b. Hot Site

This alternative provides a standby system at a separate site which can generally be accessed within hours

of a disaster. Commercial facilities have sprung up in numerous states which provide specific vendor compatible systems. For example, SUNGARD of Philadelphia, Pennsylvania has several recovery centers housing IBM 3033's and its fees range up to $5,500/month, $50,000 disaster notification fee (4 hour notice) and $8,000/day usage. COMDISCO Disaster Recovery Services Inc. charges up to $4,000/month, $10,000 disaster notification, and $4,000/day usage. These prices all vary according to the system and services provided but in general are a very expensive alternative. They are however, a quite attractive option to banks or large corporations which risk great financial loss for every hour of computer down time.

In order to be effective, the hot site must be properly configured to match the user's home system and it must be used for testing regularly to ensure continued compatibility. Any significant changes in the organization's operations must be promptly reflected in the backup site's disaster plan. It would be quite tragic to pay for a backup system with guaranteed two hour access and not be able to run the software due to incompatibility. Off-site documentation, files, systems and applications software must be kept current.

Although the hot site alternative is a very thorough means of backup, it has several drawbacks (some of which are particular to the Navy) which limit is

practicality. As mentioned before, it is very expensive and may not be cost effective in many cases. Secondly, most contracts contain an escape clause which limits the hot-site vendor's liability in the event two or more subscribers have a disaster concurrently. Basically, they try to accommodate all parties but with limited equipment facilities. This hardly seems fair since the subscriber would like a fail-safe backup plan. Of course the vendors limit the number of subscribers to one system (usually 100 or less) and reduce risk by not accepting subscribers with systems in the same building. They also try to keep the number of subscribers from the same city or power grid to a minimum. Since the larger vendors have numerous recovery centers throughout the United States, they feel that multiple disasters would not present a problem (it very well shouldn't when the client is paying more than $65,000/year for these services.) Sources at the Naval Data Automation Command, Washington, D.C. state that another problem which applies to the Navy is the duration of funding for Operation and Maintenance (O&M). Operation and maintenance, Navy funds may only be obligated in one year intervals and they are incrementally funded by Congress. This limits participation in multi-year obligation such as many of the hot-site contracts require.

c. Shared Backup Site

A third type of disaster recovery center offers a more reasonable alternative to the commercial hot site. Numerous businesses have banded together to set up their own disaster recovery centers. In this way they can share expenses and provide less expensive backup for their systems. A group of fourteen companies in Minnesota formed a corporation called Eloigne Corp. and built a recovery center in St. Paul. Although they have only a shell site, an actual hot-site could be established as well. One company, Computer Alternatives, has made a business of matching organizations with excess capacity to those needing backup. It arranges for primary and secondary backup to insure adequate coverage for its clients. This method is a bit more concrete than the previously described reciprocal agreements and has already proven its effectiveness in the case of United States Tobacco Company of Greenwich, Ct., which successfully recovered from a recent disaster. They had been backed up by Curtiss-Wright Corporation of Woodridge, New Jersey through arrangement by Computer Alternatives. This type of matching service seems like an interesting proposition for the Navy if implemented by an organization such as NAVDAC. Admittedly there may not be a lot of excess computer capacity floating around in the Navy, but this would certainly be a much more organized approach to backup than current reciprocal agreements.

Additionally, the Navy might consider setting up its own disaster recovery centers to be shared by selected significant data processing centers.

4. Automatic Data Processing Service Centers

If a thorough risk analysis has been conducted, the use of an ADP service center might be considered in light of disaster planning. In disaster planning, one is primarily concerned with the how and when of getting critical applications back on line. As discussed previously, an ideal situation would have a standby system waiting to pick up the load upon the occurrence of a disaster. This standby capability might be provided by an ADP service center through leased timesharing. Certainly it would be unreasonable to expect a service bureau to take on a disaster befallen customer with no advance notice however, a reasonable contingency plan could be worked out to provide for rapid availability of resources. One possible scheme could involve the monthly purchase of timesharing services at a level commensurate with the needs of the critical applications for a particular organization. These timesharing services could be used to run the high priority jobs at the service center while the in-house computers ran the less critical jobs (these would be pre-empted by the critical jobs in the event of a service bureau problem). The converse of this idea would probably be even more attractive

since critical applications could be kept in-house and less critical jobs contracted out. The key to this plan would be guaranteeing enough resources at the service bureau by purchasing monthly timesharing, and also ensuring that vital applications would be able to run on the service center's system. This plan is quite viable but entails precise risk analysis to identify the essential jobs and requires frequent testing to ensure compatibility of systems.

5. Documents and Vital Information for Recovery

a. Backing Up Data

It is essential that proper measures be taken to protect more than just the hardware. Without the software and data, the computer system will be of little use. Most organizations realize that replacement of software and data after a disaster would be a much more serious problem than replacement of hardware. It is quite common for software development to take hundreds of man-months of effort. Thus it would be almost impossible to re-develop any but the simplest of applications in time to stage a disaster recovery. The same logic applies to large databases and particularly to transaction files; they could be lost with no possibility of redevelopment in a major disaster. For these reasons, it is uncommon to find an organization that does not back up its software and data files. The frequency of back up is dependent upon each particular data processing

environment, but the risk analysis will indicate which files are critical and how often to dump tapes for off-site storage. Howard Schaeffer discusses database copying in greater detail in his text on data center operations [19].

b. Backing Up Documentation

Contrary to the diligence with which data processing centers usually back up their files, they are often negligent when it comes to backing up their documentation. It is likely that in the aftermath of a disaster the normal operations staff will not be completely available, and therefore documentation should be adequate for others to carry out the data processing functions. Information that is routinely kept in the data processing shop must also be safely stored elsewhere. This information includes:

--Names, phone numbers, and addresses of vendors, suppliers, and key disaster recovery personnel

--A comprehensive list and description of all equipment, peripherals, office furniture, and supplies

--Copies of written agreements and contracts

--A listing of job (application) priorities

--Operations manuals and source code

--Blueprint of physical plant layout

--List of equipment requirements in terms of electrical power, air conditioning, chill water, space, etc...

A comprehensive list of vital documents was published by the Toronto Chapter of the Association of Records Managers and Administrators [20]. The ease with which these documents can be obtained will be a critical factor in the success of disaster recovery. It would be unwise to store them in a vault which only offered access during typical nine to five weekday work hours (a disaster is not likely to abide by this timetable). Therefore it is prudent to keep copies of the disaster plan at various accessible locations (one authority suggests keeping copies of the plan in several disaster team leaders' houses - with all due regard to security considerations.) To recapitulate, the disaster recovery planning phase is virtually a waste of time unless the documents and vital information are themselves properly protected to survive a disaster.

D. CONSULTING SERVICES

1. Developing the Plan is a Fulltime Job

One inevitable question that must be answered before an organization begins development of a disaster plan is who will actualize the plan. This a difficult situation because creating the plan is a full time job; a part time effort will usually be inadequate. It is typical however, for most data processing organizations to attempt development of their disaster plans by assigning the project to an operations manager. The project becomes an overload

to the individual assigned and often takes a lower priority than day-to-day crises. Several problems occur when the disaster plan is only a part time effort. First of all, the organization must operate without a recovery plan for the duration of the development. This in itself is a compelling reason to get the plan implemented expeditiously. Secondly, if the data processing organization is undergoing any change, the disaster plan will be obsolete before it reaches completion. For these reasons many data centers have assigned a risk manager whose job it is to ensure that the risk analysis is complete and that the proper contingency planning has been executed. Not all organizations are fortunate enough to have the in-house experience and expertise necessary to carry out this function, and they should consider consulting services in order to do the job properly.

2. Advantages of a Consulting Firm

An experienced consulting firm can offer numerous advantages in developing a disaster plan. Since they will be working full time on the plan, they will be able to implement it without the encumbrance of daily operations as experienced by in-house employees. They will also have the background and prior experience which will make their efforts more efficient. Data processing organizations typically take years to come up with a usable design, whereas consultants can offer results in a matter of months.

The outside consultant may also be more credible and able to implement change in the organization. An operations manager at Davoe Raynolds Company in Louisville, Kentucky claimed,

> "I didn't have the clout to pull all the managers into a room to discuss disaster recovery, but when the consultants came and we were paying for them, all executives involved had to come."[21]

As human nature would have it, people will believe and follow the advice of an outside consultant more readily than they would believe employees. This may stem from another advantage of the consultant--objectivity. Whereas employees may not recognize poor security procedures due to acclamation to normal routine, an outside observer would not be so biased. Top level management can more easily accept a consultant's advice as unprejudiced. This can be a most important point since disaster planning will only be successful with top management support.

3. Consulting Costs

Depending on the size of the data processing operation, consultant fees range from $20,000 to over $200,000. This is usually far less than it would cost the client to produce a plan of similar quality if he attempted to do it himself. Some firms offer an economical alternative to clients who insist on providing their own manpower. The consultant provides manuals, tools, and guidance and the client does the legwork. Such an

arrangement can cost between $7,000 and $10,000. If cost is the major concern, this is very appealing; however, it loses many of the advantages of outside consultants such as objectivity, credibility, and experience.

In summary, the level of expertise available in-house will determine whether or not consulting services are needed, but it would be wise to consider their services in terms of selling the disaster plan to top level management, comparative costs, and the time necessary to implement the plan. For lists of who to contact regarding disaster and computer security planning, refer to References [21] and [22].

VI. APPLICABILITY TO NAVY ADP SYSTEMS - POLICIES AND DIRECTIVES

As previously stated, Navy ADP centers do not operate on a profit motive, so what factors can motivate them to prepare for a disaster? Basically they will be influenced by mission requirements, governing directives, and budgetary considerations. Since mission requirements will vary from center to center, it should suffice to say that each manager will have to determine how vital his data processing applications are in the scheme of overall objectives, and plan for protection of these assets accordingly. Such an evaluation would include a thorough risk analysis as discussed in Chapter V-A.

A. DIRECTIVES

Another area of influence will be the directives and policies under which Navy data processing centers must operate. The major emphasis of these directives will be discussed and the reader is referred to the documents themselves for further detail. The Government has provided some initial guidance through the Office of Management and Budget (OMB) and the National Bureau of Standards (NBS). OMB Circular A-71, Transmittal Memorandum 1 entitled, Security of Federal Automated Information Systems, directs the heads

of each executive branch department and agency to ensure that they have an adequate security program [25]. Such a security program must include a valid disaster plan for computer operations. In this circular,OMB tasked the Department of Commerce (which is responsible for the NBS) to develop and issue standards for assuring security of Automated Information Systems (AIS).

This tasking included specifying :

--Whether the standard is mandatory or voluntary

--Specific implementation actions

--Time constraints within which compliance must be made

--A process for monitoring and evaluating use

--Conditions for any waivers

These objectives had already been partially accomplished through FIPS publication 31, Guidelines for ADP Physical Security and Risk Management [12]. The General Services Administration (GSA) was tasked with enforcing security requirements including contingency planning.

The National Bureau of Standards enhanced FIPS publication 31 in 1981 with its Guidelines for ADP Contingency Planning, FIPS publication 87 [13]. These guidelines are directed toward agencies specified in OMB's circular A-71, Transmittal Memorandum 1. FIPS publication 87 is a summary of actions necessary to formulate an ADP contingency plan. It makes no claim to being all inclusive, but it is a good foundation upon which management can base its plan. Finally,

the Chief of Naval Operations, being responsible for ADP security within the Department of the Navy (DON) has issued his directive on implementation of contingency planning for Navy ADP activities, OPNAVINST 5239.1A [2]. While allowing Commanding Officers of certain activities some latitude by making them the Designated Approving Authority (DAA) of their own contingency plans, the Commander Naval Data Automation Command (NAVDAC) has been made overseer of all plans for levels I and II data.[7] This will allow NAVDAC to ensure consistency in the plans and will provide a service for technical guidance in developing the plans. All DON ADP activities were given nine months within which to execute these directives issued in August, 1982. Aside from the oversight by NAVDAC, ADP systems and their security are subject to audit by the Naval Audit Service. This may be a command requested review or may take place as part of a scheduled audit of the activity.

Whereas previous directives on ADP security and contingency planning had placed the responsibility at high levels with little or no enforcement at the field activity level, current directives have provided the technical

---

[7]Level I Data - Classified data; Level II Data - Unclassified data requiring special handling, eg. privacy act information, For Official Use Only, etc...; Level III Data - All other unclassified data.

support and have pushed the responsibility down to the proper level. The means for enforcement have been enacted, and if staffing levels permit proper auditing, violators will soon be exposed. The message and intent are clear--the CNO wants all of his ADP activities to implement and maintain comprehensive contingency plans.

B. FUNDING CONSIDERATIONS

Although the guidelines for disaster planning are clear, the means for funding it are problematic. Disaster planning does not show immediate rewards and in fact may never pay off if a disaster does not occur. Disaster plans are expensive and there is always the question of "how much is enough?" It is difficult to justify additional costs when budgets are being cut and merely meeting day-to-day operating expenses is a major concern. Another problem, inherent in the Navy's personnel assignment policy, is the short-term perspective of military employees. Disaster planning is something that keys on long-term benefits at the expense of initial significant costs. A military tour of duty lasting two to three years provides a very small window of time within which to excel. Capital intensive long-term objectives tend to make a poor impression in the short run and thus military commanders are hesitant to embark upon projects which will not bear fruit during their tenure. This

type of problem can only be alleviated by superiors who realize the sacrifice necessary to implement a disaster planning program. If the CNO's security program is indicative of policy-level sentiment in the area of contingency planning, then a positive trend is developing which will eliminate some of these problems. Finally, the execution of a risk analysis and threat survey are the basis for justifying any expenditures in disaster planning, therefore they must be thoroughly prepared and reliable. These studies will make acceptance of the budget more palatable to upper level management and enhance the arguments for instituting a disaster plan as soon as possible.

C. PROBLEMS FOR ADP SERVICE CENTERS

Although the procedure for justifying a disaster plan for one's own data processing center may be straightforward, the problem takes on a much different perspective for a service center which is running applications for numerous other activities. The risk analysis phase becomes extremely complex as the needs of many customers must be integrated into some type of cohesive disaster plan.

1. Who Conducts the Risk Analysis?

One of the Navy's regional service centers, NARDAC San Francisco, has attempted to fit its contingency plan

into the customer base by working with each customer to arrive at a dollar value for each application that it runs. This value reflects what the customer feels it would cost to replace the software, hardware, information, administrative procedures, plant/facilities, telecommunications, and personnel necessary to support his applications. While this may be a valid means of determining some index of the data center's value, it can provide very misleading information on the relative value/importance of customer applications. Therefore, this type of estimate might be useful for determining how much to spend in protecting the assets, but it is not an accurate guide for prioritizing importance of individual applications programs. For example: A small customer may depend exclusively upon the NARDAC for its data processing needs and estimate its applications at a value of $50,000. A larger activity may only parcel out a fraction of its data processing to the NARDAC and assign a value of $100,000. Which application is the most critical? If they are compared monetarily, the larger activity wins out. But what about analyzing capability to continue their missions? The small activity would be wiped out by this data processing loss whereas the large activity might suffer only minor inconvenience. Who would be to blame for such a loss? Most NARDACs believe that it is their obligation to provide contingency planning for their customers. They must keep in mind that merely providing backup for a customer's

application hardly constitutes a contingency plan. Gerald I. Isaacson, Director, Computer Security Institute's Educational Resource Center, claims that,

> "Disaster recovery planning is not a data processing problem, it's a corporate problem."
>
> "In disaster planning, you're not really trying to back up the data center, you're trying to provide survivability for the organization in the absence of the normal data center." [18]

While it is important for the data center to be involved in disaster planning, it should not bear the entire tasking nor should it assume the entire financial burden. In the case of NARDACs it is unrealistic to believe that they can fully understand their customers' mission needs and be able to integrate them all under one scheme. The users should develop their own plans and coordinate them with the NARDAC. The customer should find out how the data processing center intends to handle any contingency (from short outages up through total disaster) and plan accordingly. For instance, what priority will be given to its applications in a limited outage? While this may not constitute a disaster for the data processing center, it may do so for the user if his programs are given a low priority for processing.

Since it would be highly uneconomical for each customer to plan for its own disaster recovery center, it would be wise for them to support a scheme whereby the NARDAC had some type of a backup facility. The NARDAC

concept originated to take advantage of centralized resources and provide regional experts for data processing. This advantage should be retained by a regionalized disaster recovery plan. The complexity of such a plan would be manageable if all customers could develop their own risk analyses and assign priority to their jobs as discussed in chapter V-A-1-c. The threat analysis would be mostly conducted by the NARDAC, and the customer would coordinate loss expectancies with NARDAC.

2. Who Pays for the Plan?

In answer to the question "who pays for this service?", it would be reasonable for NARDAC to pass some of these overhead costs on to the customer. Obviously, this type of consulting and planning is a valuable service for which clients should be willing to pay. It is not a service which would necessarily be provided by a similar commercial service center and therefore would enhance the value of a NARDAC's service.

VII. CONCLUSION

This paper has raised numerous questions regarding the Navy's state of readiness in disaster planning for ADP centers. The United States government in general has become highly dependent upon computing systems. The Navy in particular, is subject to financial, organizational, mission-degrading, low-morale, and life-threatening problems when its computers fail, and therefore must ensure preparedness for computer disasters.

In the past, the Navy has placed less emphasis on disaster planning than commercial activities. Reasons for this included:

--lack of profit motive

--short-term tenure of military personnel and thus short-term goals

--lack of adequate directives

--unclear responsibility

--no high level support or enforcement

These trends are changing in large part due to high level interest in the Navy's ADP Security. There are now adequate guidelines and directives; however, it remains to be seen how well these directives will be enforced. Inevitably the axe will fall on data center managers who happen to be unprepared at the unfortunate occurrence of a

disaster. The question remains "are Navy ADP centers prepared for disaster?" Most are taking heed of the directives and contingency planning has begun, yet the efficacy of these plans remains to be seen. Realizing that preparation for a disaster does not yield immediate rewards, most managers are easing into the requirements on a limited basis and are probably doing the best that they can while staying within budgetary constraints.

To continue the momentum of high level interest, I believe that NAVDAC should sponsor a team of experts to conduct periodic assist visits in the area of ADP security and contingency planning. Under the guidance of the team, an activity could develop its plan while adhering to some type of consistent standards. The team could also help to validate current plans and ensure that they remain workable. The allowance of individual Commanding Officer discretion in approving security plans is quite appropriate; however, it would be beneficial to both the Navy and the activities for NAVDAC to have this type of oversight responsibility.

As suggested in this paper, there are numerous topics for further research on the topic of disaster planning. The areas of tactical systems and systems which process level I (classified) data require enormous security considerations when planning for disaster. The field of distributed computing may offer great potential for backing up a system but there are tradeoffs to be considered when the system is

dispersed (especially when large geographic distances are involved.)

Finally, a useful follow-up study could examine how well the Navy ADP centers have actually complied with the CNO's directives and which disaster recovery alternatives have been the most popular.

In conclusion, the following recommended reference material will provide adequate step by step guidance for Navy ADP managers to carry out the process of disaster planning in a thorough manner.

Overall Summary

(1) Shaw, James K., "An Executive Guide to ADP Contingency Planning," Draft NBS Spec Pub 500-xx, July 1981. Center for Programming Science and Technology, Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, D.C. 20234.

(2) "Disaster Recovery Just In Case," Ref. [21].

(3) "Data Security: Plan for the Worst," Ref. [22].

(4) Disaster Preparedness, Office of Emergency Preparedness Report to Congress, stock no. 4102-0006, Government Printing Office, Washington, D.C.

General Policy

(1) "Most Federal Agencies Have Done Little Planning for ADP Disasters," GAO report, Ref. [1].

(2) Security of Federal AIS, Omb Circular A-71, Transmittal Memorandum 1, Ref. [25].

Specific Navy Directives

(1) OPNAVINST 5239.1A, DON ADP Security Program, Ref. [2].

(2) Refer to appendix B of OPNAVINST 5239.1A for any directives which may be specific to a particular Navy activity.

Risk Analysis

(1) Guidelines for ADP Physical Security and Risk Management, Ref. [12].

(2) Checklists and Guidelines for Reviewing Computer Security and Installations, Management Advisory Publications, P.O. Box 151, 44 Washington St., Wellesly Hills, MA 02181 (1975).

(3) NBS Guidelines for Automated Data Processing Risk Analysis, FIPS publication 65, NTIS, Springfield, VA., 1 August 1979.

Contingency Planning

(1) Guidelines for ADP Contingency Planning, Ref. [13].

(2) "Developing a Contingency Plan," Ref. [16].

(3) OPNAVINST 5239.1A, chapter 7, Ref. [2].

LIST OF REFERENCES

1. General Accounting Office report AFMD-81-16, Most Federal Agencies Have Done Little Planning for ADP Disasters, 18 Dec. 1980.

2. Department of the Navy ADP Security Program, OPNAV Instruction 5239.1A, 03 August 1982.

3. General Accounting Office Report (Accession number 112745), Computers in Government - We Couldn't Do Without Them, June 1980.

4. Ibid. p. 6-7.

5. Ibid. p. 8.

6. Ibid. p. 18.

7. United States Public Law 95-213, Dec. 19,1977.

8. "When Computer Disaster Strikes," Business Week, p. 68, Sept. 6,1982.

9. Pollock, Kenneth A., Vulnerability of the Computer Society, Speech before the Institute of Electrical and Electronics Engineers, 1976 Conference on Cybernetics, 2 November 1976.

10. "An Evaluation of Data Processing Machine Room Loss and Selected Recovery Strategies," MISRC-WP-79-04, Working Paper Series, University of Minnesota, Minneapolis, June 1978.

11. Computers in Government, p. 9.

12. National Bureau of Standards, Federal Information Processing Standards Publication 31, Guidelines for ADP Physical Security and Risk Management, National Technical Information Service, Springfield, VA., p. 11, 1974.

13. National Bureau of Standards, Federal Information Processing Standards Publication 87, Guidelines for ADP Contingency Planning, 27 March 1981.

14. Turner, J. Crawford, Jr., "Anticipating Disaster Contains DP Damage," Data Management, p. 18-21, June 1980.

15. Gates, William E., Associate, Dames and Moore, Los Angeles, CA., Risks of Natural Hazards to Data Processing Centers and How to Reduce Potential Losses, with Emphasis on Earthquake Effects, Speech presented at Third Annual East-West Conference and Symposium on Computer Security and Disaster Recovery Planning, Newport Beach, Ca., 14-16 Feb. 1983.

16. Murray, John P., et al., "Developing a Contingency Plan," Data Management, p. 11, Jan. 1980.

17. "The Air Force Should Cancel Plans to Acquire Two Computer Systems at Most Bases," General Accounting Office report FGMSD-80-15, Oct. 26, 1979.

18. Rhoades, Wayne L., Jr., "What Good is Data Without a Computer?", Infosystems, p. 56-62, July 1981.

19. Schaeffer, Howard, Data Center Operations, Prentice-Hall, Inc. , Englewood Cliffs, N.J., p. 286-287, 1981.

20. Curry, Jack P. , " Disaster Recovery; Planning Ahead Makes all the Difference," Canadian Datasystems, p. 31, August 1981.

21. Kull, David, "Disaster Recovery Just In Case...," Computer Decisions, September 1982.

22. Harrison, Ben, "Data Security : Plan For The Worst," Infosystems, p. 58, June 1982.

23. Siewiorek, Bell, and Newell, Computer Structures, Principles, and Examples, McGraw Hill, N.Y. N.Y., p. 5, 1982.

24. Lorin, Harold, Aspects of Distributed Computer Systems, John Wiley and Sons, N.Y. N.Y., 1980.

25. "Security of Federal Automated Information Systems," Office of Management and Budget, Circular A-71, Transmittal Memorandum 1, July 27, 1978.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22314	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, California 93940	2
3.	LCDR John Hayes, Code 54HT Department of Administrative Sciences Naval Postgraduate School Monterey, California 93940	1
4.	CAPT Bradford Mercer, Code 52ZI Department of Computer Science Naval Postgraduate School Monterey, California 93940	1
5.	Naval Postgraduate School Computer Technology Curricular Office Code 37 Monterey, California 93940	1
6.	LT J.R. Hickman Navy Supply Corps School Athens, Georgia 30601	2
7.	Commander ATTN: Mr. Duane Fagg Naval Data Automation Command Washington Navy Yard Washington, D.C. 20374	1
8.	Commander ATTN: CAPT J.M. Wright Fleet Numerical Oceanographic Center Monterey, California 93940	1
9.	Mr. Bernard L. Konopko Director, Government Relations Organon, Inc. 8904 Paddock Lane Potomac, Maryland 20854	1

2

Disaster planning
for Navy ADP systems.